ОТЗЫВ
официального оппонента на диссертацию Нестеренко Алексея Юрьевича
«Математические методы обеспечения защищенного взаимодействия средств защиты информации» на соискание ученой степени доктора физико-математических наук
по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность

Целью диссертационной работы является совершенствование математических методов построения криптографических протоколов, применяемых для обеспечения защищенного взаимодействия средств защиты информации, а также методов получения обоснованных оценок безопасности криптографических протоколов.

Актуальность избранной темы подтверждается необходимостью применения криптографических протоколов при обеспечении защищенного обмена информацией в сети «Интернет», государственных информационных системах, а также для защиты критической информационной инфраструктуры Российской Федерации.

Основным критерием при выборе криптографического протокола являются обоснованные оценки мер защиты, реализуемых протоколом для обеспечения конфиденциальности передаваемой информации. Для получения таких оценок может быть использован метод, опирающийся на численные оценки сложности решения ряда математических задач, среди которых автором диссертации выделены задача нахождения дискретных логарифмов в группе точек эллиптической кривой, задача восстановления начального заполнения генератора псевдослучайных последовательностей, а также задача построения коллизии для ключевой функции хеширования. Появление эффективного метода решения одной из перечисленных задач может привести к снижению уровня безопасности криптографических протоколов, поэтому в диссертации исследуются методы построения параметров криптографических протоколов, затрудняющих решение поставленных задач.

Структура диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы, включающего 395 источников, и приложения с программами для ЭВМ. Большая часть статей, включенных в список литературы, содержит прямые ссылки на текст статьи, что существенно облегчает их поиск. Общий объем диссертации составляет 426 страниц. Во введении обоснована актуальность исследований, сформулирована их цель, описаны методы исследования, дана общая характеристика работы, сформулированы основные результаты.

В первой главе диссертации рассматриваются вопросы применения в средствах защиты информации эллиптических кривых, определенных над конечным простым полем.

Во втором параграфе главы рассматривается разработанный автором алгоритм решения задачи дискретного логарифмирования, основанный на методе Госпера поиска двух совпадающих элементов в последовательности. Доказывается теорема об оценках числа шагов данного алгоритма и приводится сравнение полученной оценки с оценками других известных алгоритмов, ведущих отсчет от известного ро-метода Полларда.

Из результатов сравнения следует, что предложенный в диссертационной работе алгоритм имеет наименьшую оценку среди рассматриваемого класса методов. Полученная оценка весьма велика и не позволяет использовать разработанный алгоритм для эффективного взлома криптографических протоколов, параметры которых определены в рекомендациях по стандартизации. С другой стороны, полученное в диссертационной работе обоснование трудоемкости метода Госпера является решением отдельной математической задачи, которая имеет собственные приложения.

В третьем параграфе первой главы рассматривается другой метод решения задачи дискретного логарифмирования в группе точек эллиптической кривой, определенной над конечным простым полем. Этот метод использует дополнительную информацию о неизвестном значении, а именно величину мультипликативного порядка неизвестного значения по модулю порядка группы, в которой решается задача дискретного логарифмирования.

Для достаточно малой доли неизвестных значений доказана теорема о существовании алгоритма, трудоемкость которого оценивается величиной порядка квадратного корня из мощности множества неизвестных значений с заданным с малым мультипликативным порядком. Данный результат не ухудшает качества семейства эллиптических кривых, используемых в действующих средствах защиты информации.

Необходимо отметить, что в отдельном разделе третьего параграфа автор диссертации приводит важную теорему, содержащую обобщение предложенного им метода. Это обобщение позволяет по-другому взглянуть на известные ранее методы дискретного логарифмирования, например, на ро-метод Полларда с ограничениями на область поиска неизвестных логарифмов, а также позволяет предъявить очень большой класс множеств, для которых может быть применен предложенный метод. При этом принадлежность секретного ключа к данным множествам может рассматриваться как дополнительная информация, знание которой приводит к компрометации криптографической схемы или протокола.

Учитывая результаты двух предыдущих параграфов, автор приводит алгоритм построения параметров эллиптических кривых, максимизирующих трудоемкость применения всех известных ему методов дискретного логарифмирования в группе точке эллиптической кривой. Вводится понятие безопасного простого числа, по модулю которого определяется эллиптическая кривая, а также формулируются требования к порядку ее группы точек. Указанные требования расширяют требования, приведенные в отечественном стандарте на электронную подпись. Автором предлагается алгоритм построения таких параметров, а также приводятся численные значения, полученные в результате практических вычислений на ЭВМ. Из этого следует, что предъявленные требования достижимы на практике, а приведенные значения могут использоваться в средствах защиты информации, успешно прошедших исследования на соответствие требованиям по безопасности.

В четвертом параграфе первой главы рассматривается другая задача, возникающая при практической реализации криптографических протоколов, а именно, задача эффективного вычисления кратной точки эллиптической кривой. Приведенный в начале главы обзор показывает разнообразие известных к настоящему моменту времени методов и, в этом ряду, автору диссертации удалось получить новые и математически обоснованные результаты.

Как известно, эллиптические кривые, применяемые в криптографических приложениях, обладают кольцом эндоморфизмов, изоморфным некоторому порядку в кольце мнимых квадратичных иррациональностей. Основываясь на идеях Г. Старка автор диссертации предложил алгоритм явного вычисления эндоморфизма эллиптической кривой, определенной над конечным расширением поля рациональных чисел. Данный алгоритм использует подходящие дроби к значениям функции Вейерштрасса и позволяет в явном виде определить коэффициенты рациональных функций, задающих эндоморфизм кривой. Предложенный алгоритм был реализован автором диссертации на ЭВМ, что позволило получить в явном виде большое число не известных ранее эндоморфизмов (примеры приводятся в тексте диссертации, а в приложении приводится код, подтверждающий корректность построенных отображений).

Надо отметить, что до работ автора диссертации было известно не более шести эндомормизмов, заданных в явном виде. Фактически, автор полностью решил проблему построения эндоморфизмов для мнимых квадратичных колец с малым значением дискриминанта. Для колец с большим значением дискриминанта данная проблема решенной

считаться не может, поскольку предложенный автором алгоритм имеет высокую трудоемкость и не может быть реализован на ЭВМ за приемлемое время.

Вторым, важным с криптографической точки зрения, результатом этого параграфа является алгоритм применения построенных эндоморфизмов для вычисления кратной точки. Для этого автором доказана теорема о разложении натуральных чисел по степеням мнимой квадратичной иррациональности, определяющей базис кольца эндоморфизмов, с заданными ограничениями на величину коэффициентов и доказана оценка на длину полученного разложения. Доказательство теоремы конструктивно и содержит в себе алгоритм, который может быть реализован на ЭВМ.

Для минимизации трудоемкости реализации построенных эндоморфизмов автором предложено использовать форму эллиптических кривых, отличную от короткой формы Вейерштрасса, которую принято применять в современных средствах защиты информации. Предъявлены соотношения, позволяющие переходить от короткой формы Вейерштрасса к построенной форме и обратно.

Во второй главе диссертационной работы рассматривается подход к построению датчиков псевдослучайных чисел, основанный на представлении действительных иррациональных чисел в заданной системе счисления. Автором выбрана шестнадцатеричная система, однако на практике могут применяться любые основания системы счисления, например, совпадающие с длиной регистра вычислительного средства. Привлекательность такого подхода заключается в том, что вырабатываемые последовательности гарантированно не имеют периода.

Применительно к данному подходу классическая теория чисел ставит две сложные математические задачи - задачу доказательства трансцендентности действительных чисел, заданных быстро сходящимся рядом специального вида, а также задачу о виде распределения коэффициентов представления таких чисел в произвольной системе счисления. Хорошо известно, что гипотеза о равномерном распределении коэффициентов числа пи является не доказанной на протяжении многих столетий.

Автор диссертации умело пользуется известными результатами в этой области, однако рассматривает несколько иную задачу, а именно, традиционную для криптографических исследований задачу определения начального значения генератора псевдослучайных последовательностей, т.е неизвестных коэффициентов действительного числа, для которого известно с заданной точностью рациональное приближение. Такая постановка задачи, применительно к разложению действительных чисел в заданной системе счисления, до работ автора не встречалась.

Для решения поставленной задачи во втором и третьем параграфах автором разработан класс алгоритмов, существенно использующих вид действительного числа. В работе рассматриваются два больших класса действительных чисел: к первому классу можно отнести число пи, а ко второму классу — число е. Для чисел из второго класса автором доказывается теорема, позволяющая не только гарантировать отсутствие периода у коэффициентов разложения, но и определяющая линейное соотношение, позволяющее представить все числа из данного класса в виде линейных комбинаций заданных констант с рациональными коэффициентами. Именно данное представление позволило автору в четвертом параграфе построить эффективный алгоритм поиска неизвестных коэффициентов. Также автором предъявлены оценки точности рационального приближения, необходимого для реализации алгоритма.

Одновременно стоит отметить, что предложенные автором диссертационной работы оценки точности рациональных приближений являются эмпирическими, т.е. подтверждаются результатами успешного восстановления неизвестных значений с помощью работы программы для ЭВМ. Разработка строго обоснования используемых оценок позволила бы поднять качество представленных в диссертации результатов на еще более высокий уровень.

В пятом параграфе предлагается подход к проведению статистического анализа вырабатываемых последовательностей и проверки гипотезы о равновероятном распределении коэффициентов вырабатываемых последовательностей.

В шестом параграфе второй главы рассматривается пример практического применения данного подхода. Приводится алгоритм аутентификации локальных пользователей средств защиты информации, использующий представления действительных чисел для выработки производного ключа аутентификации.

Третья глава диссертации посвящена разработке режима работы блочного шифра, обеспечивающего одновременное шифрование и имитозащиту обрабатываемых данных. Для разработки этого режима во втором параграфе автором построен класс ключевых функций хеширования, обеспечивающий свойство равновероятности вырабатываемых значений. Задача построения таких функций рассматривается в криптографических исследованиях более сорока лет и предложенный автором способ ее решения, очевидно, является не единственно возможным.

Автором предлагается использование линейных форм от значений нелинейных биективных отображений, применяемых одновременно как к последовательности обрабатываемых данных, так и к последовательности ключей. В диссертационной работе выявлены необходимые свойства биективных отображений и доказаны теоремы, обеспечивающие свойство равновероятности построенной функции хеширования. Доказательство теорем конструктивно, что позволяет описать классы множеств, на которых функция принимает одинаковые значения. Простота предложенного решения и использование операций, которые могут быть легко реализованы на ЭВМ, делают построенное отображение привлекательным для практического применения.

Вместе с тем, переход от предложенного отображения к режиму работы блочного шифра требует проведения дополнительных исследований. Результаты таких исследований также содержатся в тексте третьего параграфа третьей главы диссертационной работы. Автором рассмотрены атаки, как на определение секретного ключа аутентификации, так и атаки, направленные на построение коллизий к разработанному режиму, предложены алгоритмические меры защиты от указанных атак, а также проведено обоснование достаточности предложенных мер.

Четвертая глава диссертации посвящена решению задачи построения защищенного криптографического протокола из множества элементарных преобразований. Глава состоит из трех параграфов, последовательно рассматривающих вопросы построения одноразундовых или транспортных криптографических протоколов, вопросы построения многораундовых протоколов выработки общего ключа, и методику, позволяющую обосновать вероятность успешной реализации атак, направленных на компрометацию криптографического протокола.

В первом параграфе автором описывается гибридная схема шифрования, позволяющая обеспечить аутентификацию отправителя сообщения с помощью предварительно распределенного секретного ключа. Разовый ключ шифрования вырабатывается с использованием известной схемы Эль-Гамаля, реализованной в группе точек эллиптической кривой. Доказывается теорема о сведении возможности компрометации предложенной схемы к сложным математическим задачам, в частности, к рассмотренным в диссертационной работе задачам дискретного логарифмирования и компрометации датчика псевдослучайных чисел.

Во втором параграфе рассматривается подход к построению протоколов выработки общего ключа с взаимной аутентификацией субъектов взаимодействия, а также вводится понятие свойств безопасности, которые должны обеспечиваться криптографическими

протоколами. Рассматриваются такие свойства как уникальность вырабатываемого общего ключа, невозможность определения общего ключа в случае компрометации ключей аутентификации, обеспечение защиты от навязывания ключа другим субъектом взаимодействия. Приводится описание разработанного автором протокола, удовлетворяющего сформулированным свойствам и доказывается теорема о сведении выполнимости свойств безопасности к упомянутым выше сложным математическим задачам. Практическим результатом исследований, отраженных в данном параграфе стало принятие рекомендаций по стандартизации, предназначенных для защиты информации, передаваемой контрольными и измерительными устройствами.

В третьем параграфе автором формулируется расширенный список свойств безопасности, которые могут обеспечиваться криптографическими протоколами, после чего строится граф зависимостей между рассматриваемыми свойствами. Автором формулируется теоретико-автоматная модель криптографического протокола и, в рамках построенной модели, предлагается формализация рассматриваемых свойств, а также метод получения численных значений, так называемых, показателей эффективности мер защиты, реализуемых криптографическим протоколом. Следуя принятому в классическом криптографическом анализе подходу, в качестве параметров безопасности выбирается трудоемкость и вероятность успеха компрометации элементарного криптографического преобразования.

Результаты диссертации являются новыми, полученными автором лично. Они четко сформулированы и оформлены в виде строгих математических доказательств. Автореферат правильно и полно отражает содержание диссертации.

К тексту диссертации можно высказать ряд незначительных замечаний.

1. На стр. 163 излагается хорошо известный алгоритм представления рационального числа в систематическую дробь.

2. В третьей главе на стр. 219 при описании недостатков разработанного автором режима аутентифицированного шифрования используется неясный термин «структурная сложность». Стоило бы дать более конкретное определение того, что именно автор подразумевает под указанным термином.

3. На стр. 228, второй абзац сверху содержится досадная опечатка: термин «минимальная алгоритмическая сложность», должен быть заменен на «максимальная алгоритмическая сложность».

4. На стр.276 в параграфе 4.2 излагаются различные варианты разработанной автором схемы шифрования с различными эксплуатационными характеристиками. С точки зрения изложения материала было бы предпочтительнее включить в текст диссертации общую сводную таблицу, содержащую отличия между предложенными модификациями и акцентировать внимание на преимуществах одной модификации перед другой.

Заключительная оценка. Указанные замечания не умаляют значимости полученных теоретических результатов, многие из которых подтверждается практическими вычислениями с использованием ЭВМ. Диссертация Алексея Юрьевича Нестеренко на тему «Математические методы обеспечения защищенного взаимодействия средств защиты информации» имеет внутреннее единство, обладает новизной и является завершенной научно-квалификационной работой, имеющей важное практическое значение, выразившееся в учете результатов диссертации при разработке ряда государственных стандартов и рекомендаций по стандартизации.

Результаты диссертационного исследования А.Ю. Нестеренко соответствуют паспорту научной специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Диссертация соответствует критериям, определенным в пп. 2.1–2.5 «Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», предъявляемым к докторским диссертациям, а ее автор, Нестеренко Алексей Юрьевич, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Официальный оппонент
доктор физико-математических наук,
доцент кафедры информационной безопасности
факультета ВМК МГУ имени М.В. Ломоносова О.А. Логачев

11 октября 2023г.

Адрес: 119991 ГСП-1 Москва, Ленинские горы,
МГУ им. М.В. Ломоносова,
2-й учебный корпус, факультет ВМК.
email: logol@iisi.msu.ru
тел. 8(916)0376671

Подпись О.А.Логачева удостоверяю